UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,984	01/28/2000	Robert S. Eisenbart	18926-003220US	2907

20350 7590 11/03/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 09/493,984	**Applicant(s)** EISENBART ET AL.	
	Examiner Michael J. Simitoski	**Art Unit** 2134	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 05 October 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because:

Applicant's response (p. 7, ¶3) argues that signing, i.e. "generating a digital signature over data, has a specific and well-known meaning. Generally, signing data is a process of calculating a signature ..." and concludes that 'generating a signature over' means "calculating a signature using the designated data, in this case, the first and second data" and that 'generating a signature over' "does not here mean calculating a signature with one piece of data and using that signature to implicitly authenticate a second piece of data". In response to this argument, the Examiner cites Applied Cryptography, Second Edition by Schneier, a well-known authoritative reference regarding cryptography. On p. 37, Schneier discloses the simplest form of signing a document, i.e. "(1) Alice encrypts the document with her private key, thereby signing the document." Therefore, the actual process of "signing" is simply encrypting a document so that the authenticity of a document can be verified (if the decrypted version of a document is identical to the document in question, authenticity is verified because no one without the encryption key could have created the signed, i.e. encrypted, document). Similarly, "verifying" the document is accomplished by decrypting the document (p. 37, step 3). However, Schneier teaches that because public key algorithms are inefficient for signing, i.e. encrypting, long documents, Alice saves time by signing, i.e. encrypting, the hash of the document (p. 38, steps 1-4). This is, by far, the most common form of a digital signature, i.e. a digital signature is most commonly an encrypted hash of a document. This provides the same security, because if a document is modified by even one bit, on average, one half of the bits in the hash will change thereby clearly indicating a change in the original document. And the originator is also authenticated as the hash is encrypted. While applicant states that hashing does not authenticate the sender (Applicant's response, p. 8, ¶1), it is submitted that the Examiner is not relying only on a hash to read upon the claimed signature. Rather, Gennaro teaches splitting the stream into blocks, creating a table of hashes of each of the blocks and signing (encrypting) the table (p. 3). Therefore, Gennaro is creating a signature over a first and second information. With the above Schneier citations in mind, if Gennaro were generating a signature over only the hash table, as suggested (Applicant's response, p. 9, ¶2), Gennaro would create produce a one-way hash of the table and sign the hash. In fact, Applicant uses the method of Schneier, on p. 6 of Applicant's specification, a signatory group is created by hashing data and signing the hash. The data "signed" is, if read in light of Applicant's arguments (Applicant's response, p. 9, ¶2), "implicitly authenticated" if they are verified with the hash value.

Applicant's response (p. 9, ¶1) argues that in Gennaro, "only the table is signed." Again, this statement is in direct opposition to the common form of a digital signature. If read according to Applicant's interpretation, Schneier would be teaching signing a hash value, when in fact, the example document is what is being signed (Schneier, p. 38). If Applicant intends to argue that Applicant is "encrypting" the first and second data, rather than "generating a signature over" it, then recitation of these limitations must be in the claims. Further, Applicant mentions that Gennaro discloses the table being signed, "instead of signing each block". This is parallel to what the instant invention performs, in that the instant invention is not signing the first and signing the second information, but rather generating a signature over the first and second information (see for example, claim 1).

Applicant's response (p. 9, ¶4) argues that Wong discloses methods similar to those of Gennaro, in that "only the table of hash values is signed." The Examiner refers Applicant to the previous paragraph in this response. Wong's process of (in the instance of the last two packets of the first method) hashing the concatenation of a first packet with the digest of a second packet and signing the resulting hash is "generating a signature over a first information and a second information and sending the signature over the network separately from at least one of the first information or the second information". The resulting signature is a signature over both the first and second information (both blocks) and is sent separately from at least one of the blocks. Because both the digest of the second packet and the content of the first packet are hashed, both can be verified when the signature is decrypted and the signer authenticated, thereby creating a signature. Wong's process of (in the instance of the second method) hashing a list of hashes and signing it anticipates Applicant's claimed "a signature over a first information and a second information" and the signed block digest is sent separately from, for instance, the first block. Again, because the contents of both block hashes are signed, a signature is created.

Applicant's response (p. 10, ¶1-2) argues that Wasilewski's encryption of the first key with the multi-session key (MSK) and the encryption of the second key with the user's public key does not affect a signature because only the second key is signed. However, Applicant is directed to col. 9, lines 31-46 & col. 11, lines 4-48 and the rejection stated in the previous Office Action. Wasilewski discloses generating a signature/hash over first information/MSK and second information/control word (col. 9, lines 31-38) and the signature is appended to the control word (in the form of an ECM) (col. 9, lines 41-46) which is sent separately from the first information/MSK.

Applicant's response (p. 10, ¶3 - p. 12, ¶2 & p. 14, ¶4 - p. 15, ¶2) argues that the combination of Wasilewski and Banker has no supporting motivation (p. 13, ¶1) and does not teach generating a signature over a first information and a second information as recited in claim 1, authenticating the signature over the first and second information as recited in claim 8, or authorization information, wherein a signature is generated over an information object and an authorization information as recited in claim 14. However, Banker provides motivation to using an out-of-band channel by teaching that the unit will receive transmissions regardless of the tuned channel (col. 1, lines 28-44 & col. 2, lines 55-68). Further, Wasilewski discloses the alleged missing limitations of the signature over the first and second information as described previously.

Applicant's response (p. 12, ¶3 - p. 13, ¶2) argues that Shear teaches that a module may be signed multiple times, but does not disclose a signature covering more than one module. However, Wasilewski's signature is a signature over multiple objects. Shear is cited for teaching the benefits of using multiple signatures, rather than the single signature created in Wasilewski (Shear, ABSTRACT & col. 7, lines 9-18). Shear teaches that generally including multiple signatures reduces vulnerability from an algorithm compromise (Shear, ABSTRACT & col. 7, lines 9-18).

Applicant's response (p. 13, ¶3 - p. 14, ¶3) argues that Wasilewski fails to teach the limitations as argued above. However, as described above, Wasilewski '474 is cited for teaching those limitations. Wasilewski '866 is cited for teaching the inclusion of tier information in the authorization information (col. 4, lines 51-59). The motivation for modifying Wasilewski '474, as stated in the previous Office Action, is to gain the benefit of controlling access to different tiers of programs in a television subscription service.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100